Cyber Security Tip: Evaluating Your Web Browser's Security Settings

Check the security settings in your web browser to make sure they are at an appropriate level. While increasing your security may affect the functionality of some web sites, it could prevent you from being attacked.

Why are security settings for web browsers important?

Your web browser is your primary connection to the rest of the internet, and multiple applications may rely on your browser, or elements within your browser, to function. This makes the security settings within your browser even more important. Many web applications try to enhance your browsing experience by enabling different types of functionality, but this functionality might be unnecessary and may leave you susceptible to being attacked. The safest policy is to disable the majority of those features unless you decide they are necessary. If you determine that a site is trustworthy, you can choose to enable the functionality temporarily and then disable it once you are finished visiting the site.

Where can you find the settings?

Each web browser is different, so you may have to look around. For example, in Internet Explorer, you can find them by:

1. Clicking Tools on your menu bar,
2. Selecting Internet Options...,
3. Choosing the Security tab, and
4. Clicking the Custom Level button.

However, in Firefox, you:

1. Click Tools on the menu bar,
2. Select Options
3. Click the Content, Privacy, and Security tabs to explore the basic security options.

Browsers have different security options and configurations, so familiarize yourself with the menu options, check the help feature, or refer to the vendor's web site.

While every application has settings that are selected by default, you may discover that your browser also has predefined security levels that you can select. For example, Internet Explorer offers custom settings that allow you to select a particular level of security; features are enabled or disabled based on your selection. Even with these guides, it is helpful to have an understanding of what the different terms mean so that you can evaluate the features to determine which settings are appropriate for you

How do you know what your settings should be?

Ideally, you would set your security for the highest level possible. However, restricting certain features may limit some web pages from loading or functioning properly. The best approach is to adopt the highest level of security and only enable features when you require their functionality.

What do the different terms mean?

Different browsers use different terms, but here are some terms and options you may find:

Zones - Your browser may give you the option of putting web sites into different segments, or zones, and allow you to define different security restrictions for each zone. For example, Internet Explorer identifies the following zones:

- Internet - This is the general zone for all public web sites. When you browse the internet, the settings for this zone are automatically applied to the sites you visit. To give you the best protection as you browse, you should set the security to the highest level; at the very least, you should maintain a medium level.
- Local intranet - If you are in an office setting that has its own intranet, this zone contains those internal pages. Because the web content is maintained on an internal web server, it is usually safe to have less restrictive settings for these pages. However, some viruses have tapped into this zone, so be aware of what sites are listed and what privileges they are being given.
- Trusted sites - If you believe that certain sites are designed with security in mind, and you feel that content from the site can be trusted not to contain malicious materials, you can add them to your trusted sites and apply settings accordingly. You may also require that only sites that implement Secure Sockets Layer (SSL) can be active in this zone. This permits you to verify that the site you are visiting is the site that it claims to be (see Protecting Your Privacy and Understanding Web Site Certificates for more information). This is an optional zone but may be useful if you personally maintain multiple web sites or if your organization has multiple sites. Even if you trust them, avoid applying low security levels to external sites--if they are attacked, you might also become a victim.
- Restricted sites - If there are particular sites you think might not be safe, you can identify them and define heightened security settings. Because the security settings may not be enough to protect you, the best precaution is to avoid navigating to any sites that make you question whether or not they're safe.

JavaScript - Some web sites rely on web scripts such as JavaScript to achieve a certain appearance or functionality, but these scripts may be used in attacks (see Browsing Safely: Understanding Active Content and Cookies for more information).

Java and ActiveX controls - These programs are used to develop or execute active content that provides some functionality, but they may put you at risk (see Browsing Safely: Understanding Active Content and Cookies for more information).

Plug-ins - Sometimes browsers require the installation of additional software known as plug-ins to provide additional functionality. Like Java and ActiveX controls, plug-ins may be used in an attack, so before installing them, make sure that they are necessary and that the site you have to download them from is trustworthy.

You may also find options that allow you to take the following security measures:

Manage cookies - You can disable, restrict, or allow cookies as appropriate. Generally, it is best to disable cookies and then enable them if you visit a site you trust that requires them (see Browsing Safely: Understanding Active Content and Cookies for more information).

Block pop-up windows - Although turning this feature on could restrict the functionality of certain web sites, it will also minimize the number of pop-up ads you receive, some of which may be malicious (see Recognizing and Avoiding Spyware for more information).

Authors: Mindi McDowell, Jason Rafail
Produced 2005 by US-CERT, a government organization.